

KENJI M. PRICE #10523
United States Attorney
District of Hawaii

THOMAS J. BRADY #4472
Assistant U.S. Attorney
300 Ala Moana Boulevard, Rm. 6-100
Honolulu, Hawaii 96850
Telephone: (808) 541-2850
Email: tom.brady@usdoj.gov

REGINALD E. JONES
Senior Trial Attorney
U.S. Department of Justice
1400 New York Avenue, N.W., Suite 6000
Washington, DC 20005
Telephone: (202) 616-2807
Email: Reginald.Jones4@usdoj.gov

Attorneys for Plaintiff
UNITED STATES OF AMERICA

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA,)	CR. NO. 18-00069 LEK
)	
Plaintiff,)	GOVERNMENT’S TRIAL BRIEF;
)	CERTIFICATE OF SERVICE
vs.)	
)	<u>Trial</u>
GRANT MANAKU,)	Date: August 20, 2019
)	Time: 9:00 a.m.
Defendant.)	Judge: Hon. Leslie E. Kobayashi
)	

TABLE OF CONTENTS

	<u>Page(s)</u>
TABLE OF AUTHORITIES	i
I. PROCEDURAL HISTORY	1
II. FACTUAL BACKGROUND.....	2
III. STATUTE.....	9
IV. EVIDENTIARY ISSUES	10
A. Child Pornography	10
B. P2P and Child Erotica	12
C. Personal Image of Defendant’s Son	14
D. Summary Charts and Demonstratives	14
E. Other Evidentiary Issues	15
V. CONCLUSION.....	16

TABLE OF AUTHORITIES

<u>Federal Cases</u>	<u>Page(s)</u>
<i>Harris v. Gipson</i> , 2015 WL 5934735	13
<i>United States v. Becht</i> , 267 F.3d 767 (8th Cir. 2001)	11
<i>United States v. Busby</i> , 2013 WL 3296537 3 (NDCA June 28, 2013)	11-13
<i>United States v. Curtin</i> , 489 F.3d 935 (9th Cir. 2007)	12
<i>United States v. Dodds</i> , 347 F.3d 893 (11th Cir. 2003)	11
<i>United States v. Nelson</i> , 38 Fed. Appx. 386 (9th Cir. 2002)	10
<i>United States v. Presley</i> , 2008 WL 189565	13
<i>United States v. Storm</i> , 915 F. Supp. 2d 1196 (2012)	11
<i>United States v. Woods</i> , 684 F.3d 1045 (11th Cir. 2012)	16
 <u>Federal Statutes</u>	 <u>Page(s)</u>
18 U.S.C. § 2252	1, 9, 10
18 U.S.C. § 2256	9

GOVERNMENT’S TRIAL BRIEF

I. PROCEDURAL HISTORY

Defendant Grant Manaku was indicted by a federal grand jury on May 30, 2018 on one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2). The trial date is set for August 20, 2019 and expected to last 2 to 3 days with approximately 10-15 government witnesses. The pre-trial conference was held on July 22, 2019, at 1:45 p.m. before Magistrate Judge Kenneth J. Mansfield.

Motions in limine were due on July 8, 2019. The defense filed a motion in limine to limit and or exclude child pornography images. *See* Dkt. #59. On July 22, 2019, the government filed its response to defense motion in limine No. 1. *See* Dkt. #68. On July 29, 2019, this Court held a hearing on the matter, granting in part, and denying in part the motion. *See* Dkt. #72.

The government has noticed to defense two expert witnesses. For these experts, the government has provided the underlying discovery, including their CVs, reports, digital information, and has also made available the computer images and the contraband child pornography upon arrangements with investigators. Computer and forensic expert CART examiner Anthony Patrick will testify to his imaging, processing, and analysis of the laptop computer, which is the matter of the charged conduct. Computer and online child exploitation and peer-to-peer file

sharing (“P2P”) expert, Special Agent Joseph Cecchini (FBI – retired), will testify about the FBI undercover P2P operation, the analysis of the downloads in this case, and child pornography and erotica series and sites. Defendant has not noticed to the government any expert witness pursuant to Federal Rule of Evidence 702, and Defendant has not provided any reciprocal discovery.

II. FACTUAL BACKGROUND

As is routine practice, members of law enforcement assigned to child exploitation units conduct investigations on the transmission and receipt of child pornography over the internet. One of the more commonly utilized tools of child pornography traffickers are peer-to-peer file sharing networks (“P2P”). When an individual computer downloads P2P onto his or her computer, he or she then has the ability to transmit and receive any file over the internet to other users who have the same P2P software program on their computers. This is frequently used to share word processing files, software, music, video, and other files. There are many legitimate uses for P2P networks, P2P networks are also frequently utilized for the sharing of pirated copyright material and, as in this case, contraband image files such as child pornography. To assist in the detection and prevention of the trafficking in child pornography over P2P networks, law enforcement has developed investigative software that can assist in the identification of users engaged in trafficking child pornography.

Because there are numerous different P2P software programs (although most P2P programs function in the same way), law enforcement has developed many different databases and investigative programs. Once a specific user is identified, law enforcement then has the ability to work backwards and identify a suspect associated with the computer and internet protocol ("IP") address in question.

On or about Saturday, February 25, 2017, between the hours of 20:11 and Sunday, February 26, 2017 at 2:34 a.m., FBI Special Agent Joseph Cecchini, who as part of his duties was conducting an undercover computer investigation into child exploitation identified an IP address that was involved in sharing suspected child pornography files on the internet, via P2P, downloaded files previously identified as being of investigative interest to child pornography investigations from a device located at IP Address: 98.151.40.53. A subsequent review of those files revealed hundreds of both still images and videos, and included both child pornography and erotica. A few of the downloads were described in the affidavit in support of the search warrant, as follows:

a. "Pthc Toddler Girl Daphne Diaper (Tender) bum yum" is a partially downloaded video file depicting a female child laying with her shirt pulled up and her diaper opened, exposing her vagina. A male penis can be seen penetrating the vaginal lips; a whitish substance can be seen on the infant's stomach. The child appeared to be approximately three-years old.

b. "!!new!! hussyfan pthc kinderficker I ass fuck my step daughter jennifer sofie ver in bath an cum(2).avi" is a fully downloaded video file depicting a nude minor female who had not reached the age of puberty, standing in a bathtub. An adult naked male was also in the tub, standing behind the child and holding her with one arm. With his other arm, he was rubbing his penis back and forth between the child's legs. The male inserted his penis into the child's anus; the child can be heard crying. The male can be seen ejaculating on the child's stomach. The child appeared to be approximately seven-years old.

c. "Tod.mpg" is a fully downloaded video file depicting a female child who had not yet reached the age of puberty sitting on a chair with her legs spread open, exposing her vagina. She could be seen masturbating with a dildo. The child could be heard asking "how do you get the, the pictures on the ... computer?" A male replied "it's called a USB line ... I'll show you later." The child appeared to be approximately four-years old.

d. "(pthc) slave play_w_sound 4 yo cries, squirms" is a partially downloaded video file depicting a minor female, in a diaper, who had not yet reached the age of puberty, laying on her back, blindfolded or with a mask over her face. A male can be seen bending down and kissing the child. The male stood and inserted his penis into the child's mouth; he put one hand behind the child's head

and manually manipulate her head back and forth against his penis. The child could be heard crying. She appeared to be approximately three-years old.

In addition to the hundreds of images and videos of child pornography, the P2P platform in this case (known as bitTorrent) captured various data—all of which was made publically available by the host computer to share files via the BitTorrent protocol. This data included the IP address and the P2P client software being utilized by the host computer to share files via the BitTorrent protocol.

Account information obtained from TimeWarner Cable via administrative subpoena relating to IP address 98.151.40.53 for Saturday, February 25, 2017 between 20:11 and Sunday, February 26, 2017 at 2:34 a.m., revealed that the account was registered to an address located at 94-1008 Lumi Street, Waipahu, Hawaii 96797 (hereinafter “the residence”). It was determined that this household comprised of a wife and husband, an adult son, and his boyfriend, Grant MANAKU. In addition, there was one other adult son that lived at the residence.

Based on the P2P downloads, on April 24, 2017, the FBI went to Defendant’s residence to execute a federally obtained search and seizure warrant. On April 24, 2017, a federal search warrant was executed at the above address. Multiple devices were seized and subsequently examined by the FBI Computer

Analysis Response Team (CART). During the execution of the search warrant, many of the residents were interviewed, included Grant MANAKU.¹

Members of the Dela Cruz family interviewed separately and provided passwords for their respective devices. All denied downloading and/or viewing child pornography. Multiple electronic devices were seized and imaged by the FBI Computer Analysis Response Team (CART).

Grant MANAKU's April 24, 2017 Interview

Grant MANAKU acknowledged that he currently lived at the residence with his boyfriend, Brennan Dela Cruz, and had been for the past five (5) years. He was a Hawaiian Airline Flight Attendant and father of an eight (8) year old boy from a prior relationship.

Initially, MANAKU denied owning a laptop computer, twice. When confronted about the Dell Inspiron Laptop computer found in his shared bedroom closet, MANAKU admitted that it was his laptop computer and added that the laptop had been “broken” for several years and that he had stored his resume in a document folder. MANAKU denied ever seeing child pornography or knowing anyone else that viewed child pornography.

¹ Apprised of Constitutional rights, MANAKU waived them and provided a statement. MANAKU had provided statements to agents twice that morning – the first occurrence outside the residence and the second occurrence inside the residence.

The Dell Inspiron laptop computer containing child pornography was found in the bedroom closet shared by Grant MANAKU and Brennan Dela Cruz.

Digital Evidence Laboratory Report of Examination (DELREX)

The only electronic device seized from the Dela Cruz residence on April 24, 2017 that contained child pornography was found on a Dell Inspiron 15-3521 laptop computer, bearing Serial Number 6B0LIX1, the same laptop found in Grant MANAKU's bedroom closet. FBI Forensic Examiner Anthony William Patrick made the following findings:

- the user generated user account:
 - User name: grant
 - SID Unique Identifier: 1001
 - Full Name: grant manaku (upon further review, it was found that the operating system was Windows 10 Home and the computer has a registered owner of gmanaku@hotmail.com. In addition, there was a picture icon of Grant MANAKU's son associated with this address).
- Twenty-six (26) instances of searches for child pornography/erotica. (The search terms included, but not limited to “pthc”, “pedo”, “bibicam boy”, etc...).

- During the Case Agent Investigative Review (CAIR) process, all graphic and video files run through a list of known child pornography provided by the Digital Analysis and Research Center (DARC). The results were:
 - 537 graphic files were pre-selected by DARC as child pornography;
 - 167 graphic files were pre-selected by DARC as child exploitation;
 - 4,813 graphic files containing child pornography;
 - 206 video files containing child pornography.

Of note is that the final Computer Analysis Review Team (CART) report was significantly delayed due to technical issues regarding the recovery of the images from the device. Specifically, many of the images were deleted and recovered through the process of “carving.”² Content of the videos includes material for several guideline enhancements.

Grant MANAKU’s May 1, 2017 Contact with Law Enforcement

On May 1, 2017, FBI agents went to Grant MANAKU’s residence located at 94-1047 Oli Place, Apartment F6, Waipahu, Hawaii 96797. MANAKU was living there with his mother as well as two other disabled relatives. MANAKU’s mother

² File carving is the process of reassembling computer files from fragments in the absence of filesystem metadata. When a file is deleted, only the entry in the file system metadata is removed, while the actual data is still on the disc. After a format and even a repartitioning it might be that most of raw data is untouched and can be recovered using file carving.

indicated that her son Grant MANAKU had been living with her since a recent disagreement with the Dela Cruz household. MANAKU advised that he felt he should “talk with an attorney” prior to speaking to the FBI and the interview did not take place.

After the FBI conducted a forensic analysis on the computers and reviewed the contents, the present indictment was returned against the defendant for one count of possession of child pornography pertaining to images found on the laptop. The forensic examination and review of the files on the laptop revealed that, at the time of the undercover download of images to the seizure of the laptop, there were hundreds of images of child pornography in Defendant’s master files and many additional images in carved and inode files.

III. STATUTE

The indictment alleges that Defendant knowingly possessed child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Specifically, on or about and between February 25, 2017, and April 24, 2017, both dates being approximate and inclusive, within the District of Hawaii, Defendant knowingly possessed material that contained images of child pornography, as defined in Title 18, U.S.C. § 2256(8)(A), that involved the use of one or more prepubescent minors, and minors who had not obtained 12 years of age, and that had been mailed, shipped, and transported in interstate and foreign commerce. Generally, to prove the

offense beyond a reasonable doubt, the jury must find that at least one visual image depicting at least one minor engaged in sexually explicit conduct, and Defendant knew of such visual image and that it depicted such conduct of a minor. The indictment includes the aggravating statutory penalty that at least one of the visual depictions were of a minor under the age of 12, in violation of 18 U.S.C.

§ 2252(b)(2). The parties filed joint proposed jury instructions on August 7, 2019, to cover the elements and definitions of this charge.

IV. EVIDENTIARY ISSUES

A. Child Pornography

The subject matter of the case involves child pornography. For the government to prove its case beyond a reasonable doubt, it needs to show the jury a sample of the images that were on the computer. This is critical to prove the elements of knowledge and a minor under the age of 12. The government has chosen a sample of the child pornography based on the image, date of import over time, and location in the computer, which are essential to proving Defendant's knowledge, and dominion and control over the computer. *See, e.g., United States v. Nelson*, 38 Fed. Appx. 386, 388-89 (9th Cir. 2002) (admission of 14,000 sexual depictions, including "hundreds, if not more than one thousand" child pornographic images, was harmless error because they were properly before the court and in light of overwhelming evidence of receipt and possession). The images

themselves need to be viewed for the jury to understand the stark difference amongst pornographic images and that there could be no accident or mistake between the volume of adult pornography and the illegal child pornography on the computer. *See, e.g., United States v. Dodds*, 347 F.3d 893, 898 (11th Cir. 2003) (government introduced 66 child pornography images, among other related evidence); *United States v. Busby*, 2013 WL 3296537, at *3-4 (NDCA June 28, 2013) (Rule 403 does not dictate total image count). The images were contained in different parts of Defendant's computer, including the Photos Library, iPhotos Library, import files, and carved files in the computer's unallocated space.³ The government does *not* propose showing the jury the same image multiple times, which could be duplicative, but instead will explain to the jury where a particular image shown is contained in the computer.

Generally, the government has the discretion to choose which evidence to present and how to present it. *United States v. Becht*, 267 F.3d 767, 770 (8th Cir. 2001) ("absent the unusual circumstance of prior criminal status, the Government

³ Defendant had images of child pornography and child erotica in the unallocated space on his computer, which are known as "carved" files. The district court in *United States v. Storm*, 915 F. Supp. 2d 1196 (2012), admitted child pornography images in the unallocated space of the computer because those images were probative of intent and knowledge. Those images were emptied from the operating system's trash or recycle bin, but were once on the computer's hard drive. *Id.* at 1202, n.2. The government intends to introduce a representative sample image from the carved files.

is free to offer its evidence as it sees fit"). It is only reasonable that, since the government must carry the burden of proof at trial, it be afforded reasonable leeway in determining the most effective ways to present evidence, in particular affirmatively choosing only a sample of the evidence to show the jury.

The selected images are contraband and although they are identified, the images cannot be turned over as part of the exhibit list. The descriptions are included and the images have been and are available for viewing by the defense upon arrangements with investigators. In addition, the government will make arrangements for the Court to view the images prior to admission at trial. *See United States v. Curtin*, 489 F.3d 935 (9th Cir. 2007).

B. P2P and Child Erotica

The government took the same selective approach for the P2P downloads on the subject computer and child erotica located on the laptop. These videos and images are also available to the defense for viewing and to the Court. For the P2P downloads, the government intends to introduce the descriptive names of the videos that were downloaded and available on the subject computer and described in the government's Rule 404(b) notice and filing.⁴ *See* Dkt. #68 at 6-11. *See*,

⁴ The P2P evidence satisfies the prongs of admission pursuant to the Ninth Circuit test. The evidence is critical to the element of knowledge and has a strong connection to Defendant. In a more extreme example involving a more tenuous connection to the defendant, an Eastern District of California district court admitted extrinsic evidence of representative child pornography images from

e.g., *Busby*, 2013 WL 3296537, at *3-4, 6, 9 (prior sexual molestation and P2P file logs with sexually graphic names admissible to show knowledge and “provide the jury with a logical and complete picture of the events leading to [child pornography] charge,” and not unfairly prejudicial). The government’s expert will explain that the names and full downloads all appeared and were available on the subject computer itself such that the subject computer was able to share these files with the FBI undercover computer and then download the relevant data. At trial, rather than introduce all the videos, of which some are over twenty minutes, the government intends to show only a clip of the videos downloaded by the undercover computer. The selected images of child erotica were chosen to illustrate a series, watermarks, and based on location on the computer and date of import over a period of years. *See, e.g.*, *United States v. Presley*, 2008 WL 189565, at *2 (WDWA Jan. 16, 2008) (child erotica probative to suggest knowledge); *Busby*, 2013 WL 3296537, at *4 (discussing the probative value of showing series or photosets shown to the jury in sequence involving child erotica and child pornography that are not cumulative and “tell a full story regarding

webpages accessed by the defendant even through there was no proof that the defendant actually viewed any of the images. *Harris v. Gipson*, 2015 WL 5934735, at *5-6 (EDCA Oct. 9, 2015). The court concluded that there was a reasonable inference that the defendant was sexually interested in preteen girls by seeking out the internet webpages. *Id.* Moreover, the P2P evidence here is not unfairly prejudicial since the government does not intend to introduce every video from Defendant’s IP address in full length and proposed a limiting jury instruction.

Defendant's conduct"). This evidence is highly probative to show dominion, control, knowledge, state of mind, plan, identity, and absence of mistake or accident.

C. Personal Image of Defendant's Son

The government will seek to introduce evidence at trial of a single image of Defendant's son to prove possession, dominion, control, and knowledge. The image of Defendant's son, contained in a user created folder, is the profile image.⁵ This personal image is probative of the defendant's use of the computer. The user has to manually place the profile photograph in his laptop computer. The timing of the imports, source, and creation also are probative of defendant's knowledge of the child pornography.

The image of Defendant's son that is on the laptop are similarly probative of possession and knowledge. Specifically, the government intends to introduce at least one image of Defendant's son from the laptop.

D. Summary Charts and Demonstratives

The government will introduce summary charts and demonstratives as part of its case-in-chief and during arguments. Defendant has all the underlying evidence, which was produced in discovery. All final charts and demonstratives

⁵ This image is non-pornographic with the words "Grant Manaku" below the image.

will be produced to Defendant for review prior to their introduction at trial. Most of the charts and demonstratives will be used during the testimony of the government's experts. Summary charts and demonstratives will be used to expedite, focus, and clarify Special Agent Anthony Patrick's testimony about the laptop computer. Rather than introduce the entire imaged computer and data to then painstakingly sort through the evidence, Special Agent Patrick will walk through demonstratives explaining his analysis and testing, and summary information pertaining to relevant information on the computer. Former Special Agent Joseph Cecchini will use a demonstrative to explain the undercover process in connecting on P2P and to demonstrate how P2P functions.

E. Other Evidentiary Issues

During the testimony of FBI Special Agent Robert King, he will explain how he identified and selected the images of child pornography. As part of the investigation, he identified known victims by submitting the evidence to the National Center for Missing and Exploited Children (NCMEC). NCMEC issues a report of known victims, including their personal information, the circumstances of their victimization, and the law enforcement officer responsible for the case. In this case, multiple images of child pornography on the laptop computer were identified by NCMEC. Although the report is generally hearsay evidence, the reference to the contents of the report is admissible when offered to explain why

certain images were selected for in-depth analysis. *See, e.g., United States v. Woods*, 684 F.3d 1045, 1062 (11th Cir. 2012).

V. CONCLUSION

Proving Defendant's state of mind, knowledge, preparation and identity in committing the crimes charged are critical to the quest for truth in this case. In *Huddleston*, for extrinsic evidence, the Supreme Court recognized the necessity of other acts evidence in cases like this and emphasized the low threshold of relevance that the proponent must establish. The government has exceeded the required relevance threshold in the instant case and refuted any claim that the probative value of this evidence is substantially outweighed by its prejudicial effect. Accordingly, the government respectfully requests that this court deem the prior acts evidence admissible under Rules 404(b) and 403 as well as intrinsically intertwined evidence which is directly connected to the factual circumstances of the charged crime and provides contextual or background information to the jury.

CERTIFICATE OF SERVICE

I hereby certify that, on the date and by the method of service noted below, a true and correct copy of the foregoing was served on the following at their last known address:

Served Electronically Via CM/ECF:

PETER C. WOLFF, JR.
Federal Public Defender

peter_wolff@fd.org

Attorney for Defendant
GRANT MANAKU

DATED: August 7, 2019, Honolulu, Hawaii.

/s/ Jodene Isa
Legal Assistant
U.S. Attorney's Office